Oluwole Adewumi Adewusi

Research Associate, CyLab-Africa (Upanzi Network), Carnegie Mellon University
oluwole.adewusi@gmail.com | *olusecc.github.io* | *linkedin.com/in/olusecc*

RESEARCH SUMMARY

My research focuses on the gap between how security systems are designed and how they behave once deployed: how users interact with them, how attackers exploit them, and how operational constraints shape both. I work across usable security, adversarial systems, agentic AI for security operations, and open-source security infrastructure, combining empirical study of real-world deployments with adversarial proof-of-concept development and the engineering of systems that hold up in production use.

EDUCATION

Master of Science, Information Technology May 2025
Carnegie Mellon University. Cumulative GPA: 3.85 / 4.0.

Bachelor of Engineering, Electrical and Electronics Engineering June 2019
Kwara State University, Malete, Nigeria. .

RESEARCH INTERESTS

Security of agentic and multi-agent AI systems; trust boundaries and structural guarantees in agent architectures; usable security and privacy in low- and middle-income contexts; AI-driven security operations; security of critical digital infrastructure; digital forensics automation.

RESEARCH AREAS

1. Payment Verification Practices and Security Gaps in Mobile Money

Merchants in Rwanda rely on a verification step that exists nowhere in the mobile money system's intended design: the merchant inspects the customer's screen and decides whether to release goods. This work characterises that practice and the security property it violates.

- Studied how Rwandan merchants verify mobile money payments through a qualitative interview study, finding a systematic gap between the operator's intended confirmation workflow and merchants' actual verification behaviour, with the authenticity of proof-of-payment as the security property under threat.
- Conducted under both institutional IRB and Rwanda National Ethics Committee approval(RNEC). Paper accepted to USENIX Security 2026.

2. Adversarial Payment Confirmation Attacks on Mobile Money Systems

A follow-up to Area 1 above: how cheaply and effectively can an adversary fabricate the visual evidence merchants rely on? This work builds and tests a working attack, then measures whether merchants can detect it.

- Built a proof-of-concept Android attack that replicates the mobile money payment workflow, performs AccessibilityService-based merchant enumeration, monitors SMS via regular-expression filtering, and dispatches forged confirmation messages through a third-party SMS gateway.
- Designed a controlled user study measuring whether merchants can distinguish real from forged confirmations, with time-to-detection and verification behaviour as primary measures.
- Coordinated responsible disclosure to MTN Rwanda and Airtel Rwanda under IRB and RNEC approval.

3. Authentication Design and Security in Mobile Money Systems

Most digital identity systems assume reliable internet, modern smartphones, and one user per device. None of these hold for the populations e-government systems in Sub-Saharan Africa are meant to serve. This work treats authentication as a distributed systems problem under those constraints.

- Designed a hybrid authentication framework combining USSD-based multi-factor authentication (SIM verification, PIN entry, session token binding) with cryptographically bound JSON Web Tokens for session continuity under intermittent connectivity.
- Built a STRIDE threat model covering SIM swapping, phishing, eavesdropping, session hijacking, denial of service, and privilege escalation, with extensions for shared-device usage and region-specific social engineering.

- Evaluated against OAuth-based Single Sign-On under controlled network impairment: 45% lower authentication time, 15% higher success rate under poor connectivity, and session integrity maintained across 98.5% of simulated network disruptions. Presented at PST 2025; poster at IEEE S&P 2025.

4. Agentic AI and Automation for Security Operations

This area covers two strands of work on applying AI and automation to security operations, with trustworthiness and the analyst-in-the-loop as the central concern.

- Building an independent multi-agent security operations system with a coordinator-worker architecture, where a coordinator decomposes alert investigation across worker agents, with cost guardrails and agent-layer observability designed in from the start.
- Contributing to the design of a vendor-neutral AI-driven SOC architecture for Digital Public Goods (MOSIP, DHIS2, Mojaloop, OpenData), using OCSF as a normalisation schema and Sigma as the detection layer, with platform-native packaging for Elastic, Splunk, Sentinel, and QRadar.

5. Digital Forensics Automation for Resource-Constrained Security Teams

Most security teams outside well-funded enterprises operate without the commercial forensic and SIEM platforms the field's tooling assumes. This work designs and operates an integrated open-source DFIR pipeline that gives under-resourced teams equivalent investigative capability.

- Built a continuous-integration-orchestrated DFIR pipeline integrating SleuthKit, Plaso, bulk_extractor, Volatility3, YARA, IRIS, MISP, and the ELK stack across a multi-server architecture, orchestrated via Jenkins reducing investigation cycle time by an estimated 60% against manual workflows. Open source: *github.com/olusecc*.

PUBLICATIONS AND SCHOLARLY ACTIVITY

Peer-Reviewed Conference Papers

- **Oluwole Adewusi**, Wallace S. Msagusa, Jean Pierre Imanirumva, Okemawo Obadofin, Jema D. Ndibwile. *Beyond SSO: Mobile Money Authentication for Inclusive e-Government in Sub-Saharan Africa.* Proceedings of the 22nd Annual International Conference on Privacy, Security and Trust (PST), Fredericton, Canada, 2025.
- **Oluwole Adewusi**, Assane Gueye, Wallace S. Msagusa, Jema David Ndibwile, David Nkundineza, Okemawo Obadofin, Wilson Rutaremara, Blase Ur. *Security and Privacy Considerations for Confirming Payments in Rwandan Mobile Money Systems.* Accepted, 35th USENIX Security Symposium, 2026.

Conference Poster

- **Oluwole Adewusi** et al. *Leveraging Mobile Money Authentication for Inclusive e-Government in Sub-Saharan Africa* (poster). IEEE Symposium on Security and Privacy (IEEE S&P), San Francisco, 2025.

Paper in Draft

- *Payment Confirmation Attacks on Mobile Money.* In draft, co-authored with. Blase Ur (University of Chicago). Android proof-of-concept exploit against the payment verification gap, conducted under IRB and RNEC approval.

RESEARCH AND PROFESSIONAL EXPERIENCE

Research Associate, CyLab-Africa (Upanzi Network), CMU Aug 2025 – Present

- Conduct research on adversarial payment confirmation attacks against mobile money systems, including proof-of-concept development, controlled user studies, and responsible disclosure to MTN and Airtel Rwanda under IRB and RNEC oversight.
- Co-author active research with Prof. Blase Ur (University of Chicago) on fake payment attack characterisation, detection, and mitigation design.
- Build and operate an open-source DFIR platform integrating ten specialist tools across a multi-server architecture; contribute to the design of a vendor-neutral AI-driven SOC architecture for Digital Public Goods.

Graduate Teaching Assistant, Network Security & Ethical Hacking, CMU Jan 2024 – May 2025

- Supported delivery of graduate-level Network Security and Ethical Hacking courses to 50+ students; designed labs, supervised student projects, and mentored students through certification pathways.

Cybersecurity Analyst, Spottoball Limited (Remote) Apr 2022 – Dec 2023

- Operated SIEM-based security monitoring processing roughly 200 GB of daily logs; led incident response investigations and maintained compliance documentation.
- Executed vendor security assessments using NIST and MITRE ATT&CK frameworks across 12 critical vendors.

IT Analyst, Zheel Limited, Lagos, Nigeria Sep 2020 – Mar 2022

- Conducted security assessments following CIS and NIST frameworks, identifying 45+ previously undetected vulnerabilities and contributing to a 65% reduction in compliance gaps.

Adjunct Instructor, Yaba College of Technology, Lagos, Nigeria May 2018 – Apr 2019

- Delivered undergraduate cybersecurity and network security courses; developed curriculum incorporating threat intelligence and certification pathways.

TECHNICAL SKILLS

Programming: Python (primary), Bash, Groovy (Jenkinsfiles), Java and Kotlin (Android), JavaScript.

Security: DFIR (Volatility3, SleuthKit, Plaso, YARA, bulk_extractor); SOC tooling (Elastic, Splunk, Sentinel, QRadar, Sigma, OCSF); threat intelligence (MISP, IRIS); threat modelling (STRIDE); penetration testing.

AI and ML: LLM orchestration and tool use, agentic system design, prompt engineering, retrieval-augmented patterns, local inference (Ollama, llama.cpp); working familiarity with PyTorch and Hugging Face for applied tasks.

Infrastructure: Kubernetes, Docker, Terraform, Ansible, Jenkins, GitHub Actions, GCP, AWS.

CERTIFICATIONS

Hold: CompTIA Security+ CE; AWS Certified Solutions Architect Associate (SAA-C03); Microsoft SC-900; Microsoft SC-200; Linux Foundation KCNA.

In progress: CISSP (ISC2); CISM (ISACA); ISO 27001 Lead Implementer (PECB); CKA, CKAD, CKS (Linux Foundation).

LANGUAGES

English (full professional proficiency).

REFERENCES

Dr. Jema D. Ndibwile
Assistant Teaching Professor Carnegie Mellon University.
Email: jndibwil@andrew.cmu.edu | Relationship: senior author on Beyond SSO, practicum advisor, and research supervisor at Upanzi.

Edwin K. Kairu, CISSP
Adjunct Teaching Instructor Carnegie Mellon University.

Email: ekairu@andrew.cmu.edu | Relationship: Instructor, collaborator and mentor.